Voltage Stability Constrained Moving Target Defense against Net Load Redistribution Attacks

Hang Zhang, *Member, IEEE*, Bo Liu, *Member, IEEE*, Xuebo Liu, *Member, IEEE*, Anil Pahwa, *Fellow, IEEE*, and Hongyu Wu, *Senior Member, IEEE*

***Abstract*—Moving target defense (MTD) using distributed flexible AC transmission system (D-FACTS) devices is a promising defense strategy to detect stealthy false data injection (FDI) attacks against the power system state estimation. However, all existing studies myopically perturb the reactance of D-FACTS lines without considering the system voltage stability. In this paper, we first illustrate voltage instability induced by MTDs in a three-bus system. To address this issue, we further propose a novel MTD framework that explicitly considers system voltage stability by using continuation power flow and voltage stability indices. We mathematically derive the sensitivity matrix of voltage stability index to line impedance, on which an optimization problem for maximizing voltage stability index is formulated. This framework is tested on the IEEE 14-bus and the IEEE 118-bus transmission systems, in which net load redistribution attacks are launched by sophisticated attackers. The simulation results show the effectiveness of the proposed framework in circumventing the voltage instability while maintaining the detection effectiveness of MTD. We conduct case studies with and without the proposed framework under different MTD planning and operational methods. The impacts of the proposed two methods on attack detection effectiveness and system economic metrics are also revealed.**

***Index Terms*—Moving target defense, voltage stability, load redistribution attack, continuation power flow, false data injection, state estimation**

I. Introduction

The landscape of smart grid, arguably one of the most complex cyber-physical systems in history, is undergoing a radical transformation [1]. Increasing renewable energy resources, integration of information and communication technologies have organized a universal cyber-infrastructure interwoven with the bulk power system, making it susceptible to cyber-physical attacks. A wide variety of motivations exist for launching such attacks, ranging from economic reasons, terrorism to grudge (a disgruntled employee). The U.S. Department of Energy received 368 power interruption reports related to cyber-physical attacks between 2011 and 2014 [2].

The concept of moving target defense (MTD) has been introduced in the smart grid in the face of emerging cyber-physical attacks [3], [4]. MTD proactively perturbs the transmission line impedance using distributed flexible AC transmission system (D-FACTS) devices to invalidate attackers' knowledge about the power system configurations. Without knowing the true power system configuration, it is difficult for an attacker to construct stealthy false data injection (FDI) attacks against power system state estimation [1], [5]–[9]. The recent proliferation of D-FACTS devices [10] has attracted increasing research attention due to their add-on cyber-physical security benefits via MTD.

The majority of MTD strategies in the literature are designed to detect FDI attacks against state estimation [6], [8], [9], [11]. Liu et al. [12] first propounded that there are two intertwined and essential problems associated with MTD, i.e., MTD planning and MTD operation. The MTD planning refers to optimally install MTD devices (e.g., D-FACTS devices) on an appropriately identified subset of the system (e.g., transmission lines). The MTD operation determines how to optimally dispatch MTD device setpoints in real-time. A random MTD (RMTD) operation [11] was proposed to randomly change the reactance of D-FACTS equipped transmission lines without considering the detection effectiveness. A DC optimal power flow (OPF) based MTD operation [13] was proposed to minimize the generation cost while ensuring MTD detection effectiveness. An AC-OPF based optimized MTD (OMTD) strategy that minimizes the system loss is introduced in [5]. In [7], Stuxnet-like attacks, which can compromise the control signals to mislead the system to unsafe conditions and inject false sensor measurements to cover the ongoing attack, were detected by MTD. Liu et al. [14] defined the "hidden" MTD (HMTD) which optimally changes the branch reactance in AC network to minimize the system loss as well as line power flow differences. An HMTD is stealthy to attackers, even when the attackers are capable of checking the activation of D-FACTS [6]. In [15], Cui et al. proposed an HMTD strategy for three-phase unbalanced distribution systems. Lakshminarayana et al. [16] proposed to actively perform MTD, thus, the attacker's knowledge to mask the effects of the physical attack is outdated.

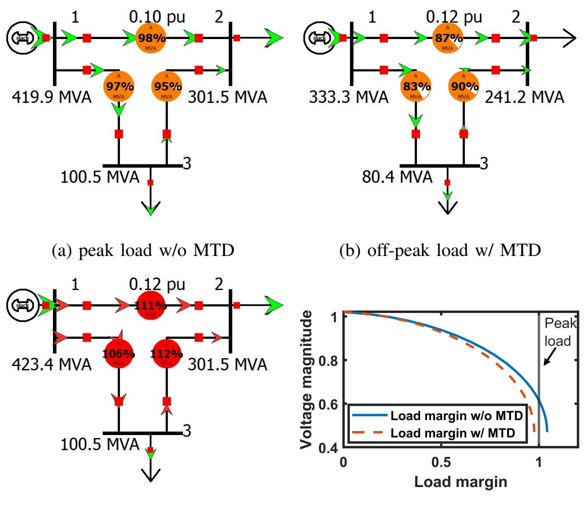
However, MTD operations may deviate the steady-state operating point of a power system from its optimal one, causing massive economic and stability impacts [5]. In [17], the voltage stability is defined as the ability of a power system to maintain steady voltages at all buses in the system after being subjected to a disturbance. One of the most common disturbances is the load increases which occur due to the peak load period. To maintain stability after such disturbance, the system needs the preserved capabilities of transmission network for power transfer. The action of MTD perturbation which changes the transmission line impedance may degrade the capability of the power transfer and cause voltage collapse during peak load period. Wang et al. [18] proposed an online line switching methodology for increasing load margins to static stability limit of a look-ahead power system. Cui et al. [19] proposed a voltage stability constrained OPF model utilizing a sufficient condition on power flow Jacobian nonsingularity. Wang et al. [20] proposed a voltage stability constrained OPF by using the minimum singular value of the power flow Jacobian as a voltage stability index. To the best of our knowledge, there is no research on MTD operation to detect FDI attacks while guaranteeing system stability. Furthermore, even if existing

MTD operational approaches [15], [16], [21] are proposed to follow some security constraints such as power flow limits and safe voltage boundaries, all those approaches consider a single-hour system load without taking into account forecasted load variations in look-ahead time periods. This might be plausible for AC OPF since it is frequently implemented, e.g., on an hourly basis. However, the frequency of the MTD can be several hours to a few days depending on the attacker's capabilities as well as how a system operator executes it (e.g., an event-based MTD strategy [22]). The lack of such look-ahead capabilities in existing MTD methods may cause system instability or even voltage collapse due to the reduction of load margin or voltage stability degradation between two consecutive MTD executions.

This paper aims to fill the gap by proposing a novel voltage-stability-constrained MTD framework against highly structured FDI attacks especially in the presence of stressful system conditions. One important consideration here is that the voltage-stability improvement ought to be minimally "invasive", meaning such an enhancement should not significantly degrade the attack detection effectiveness of the MTDs or incur a prominent increase in the system operating cost. The contributions of this paper are described as follows:

- We reveal through a 3-bus system that a system with the existing MTD operation methods can suffer voltage instability or even experience voltage collapse at the peak load.
- We propose a voltage stability (t-index) optimization method to enhance the original MTD strategies. Specifically, we mathematically derive the sensitivity matrix of the voltage stability index with respect to line impedance. The proposed optimization method maximizes the lowest index value among all the load buses with the minimum impedance adjustment; therefore, the system voltage stability is considered while the impact on the original MTD strategy is minimized.
- We develop a load margin constrained method based on Continuation Power Flow [23] (CPF) to ensure a sufficient load margin for system voltage stability at the most stressful time period. The power injection to impedance sensitivity is utilized to calculate safe MTD setpoints adjustment with ample load margins.
- We present a new MTD framework that seamlessly integrates the above two voltage stability constrained methods into the original MTD operational methods. Case studies on IEEE 14-bus and 118-bus systems are conducted to test the proposed MTD framework against one of the most sophisticated FDI attacks, i.e., net load redistribution attacks.

The rest of this paper is organized as follows. In Section II, we use a 3-bus toy system to show an MTD operation without look-ahead capability can degrade the power transfer capability and cause voltage instability at peak load. Preliminaries and related work are provided in Section III. The two MTD adjustment methods are proposed in Section IV. Case studies are in Section V and conclusions are drawn in Section VI.



(a) peak load w/o MTD (b) off-peak load w/ MTD

(c) peak load w/ MTD (d) Nose curves at peak load

Fig. 1. MTD-induced voltage instability in the 3-bus system

II. MTD-Induced Voltage Stability Issues

In this section, we show the voltage instability issue induced by existing MTD methods in a 3-bus system. Figure 1 illustrates this system, in which Bus 1 is the slack bus with a generation capacity of 500 MVA. Buses 2 and 3 are load buses where the off-peak load are 241.2 MVA and 80.4 MVA, respectively. The load increases by 25% from the off-peak hour to peak hour. The limits of Lines 1-2, 1-3, and 2-3 are 210 MVA, 210 MVA, and 100 MVA, respectively.

Assuming it is an off-peak hour, the system without MTD is in a normal steady-state and so is the system at the peak load as shown in Fig. 1(a). When an MTD is introduced at the off-peak load, e.g., the impedance of Line 1-2 changes from 0.1 to 0.12 per unit, the MTD constructed at the off-peak load would not cause any operational issues (see Fig. 1(b)) since all MTD-ACOPF constraints are satisfied in the existing models [5], [24]. However, this is not the case when it comes to the peak load. It is seen in Fig. 1(c) that all line flow limits in the system are violated. Figure 1(d) further compares nose curves with and without MTD. A nose curve represents the maximum power transfer that the system can handle given a specific system configuration (line impedance). As seen, the nose point without MTD is to the right of a vertical peak load line, whereas the nose point with MTD is to the left of the peak load. Figure 1(d) suggests that the load margin decreases with the MTD implemented at the off-peak hour and the system will suffer voltage instability issue at the peak hour.

The above issue resides in existing MTD methods that myopically perturb the line impedance without looking-ahead capabilities in the MTD rolling window for reserving sufficient load margin. The lack of such capability in existing MTD models may lead to insufficient margin for power transfer and voltage support [17]. In reality, power systems are much more complicated than this example of a 3-bus system. Thus, voltage stability issue ought to be systematically addressed for any realistic applications of MTD methods, particularly in the presence of drastic net load variations caused by an increasing amount of renewable generation. To distinguish the system operation point with or without MTD, we define hereinafter the D-FACTS operation point before MTD as *pre-MTD*, while the operation point after MTD as *post-MTD*.

III. Preliminaries

In this section, we introduce background knowledge of net load redistribution attack, MTD, power injection to impedance sensitivity matrix, and voltage stability index t as preliminaries.

A. Net Load Redistribution Attack

To bypass the detection mechanism, the FDI attack vectors need to be consistent with the physical characteristics of the attacked power system [25]. Yuan et al. [26] for the first time proposed a special case of FDI attacks, i.e., load redistribution (LR) attack. With the increasing penetration of renewable-based distributed energy resources (DERs), the malicious manipulation of net load measurements (load minus DER generation) at DER buses can be disguised as the renewable generation uncertainty. Therefore, considering the attacker's practical capability of manipulating the net load measurements, we introduced an improved LR attack strategy, namely net load redistribution attack [27]. The goal of the net load redistribution attack is to mislead the AC state estimation with an illusory over- or under-voltage issue by injecting highly-structured attack vectors into the measurements. To bypass the BDD, the net load redistribution attack stealthiness constraints pertaining to boundary conditions between the attack and non-attack areas were proposed. Those constraints included restrictions on voltage magnitude measurements on the boundary buses and power flow measurements on the tie lines. With the required local information within the attack region and the stealthiness constraints, the net load redistribution attack is modeled as an AC-OPF problem for attackers, in which the prevailing AC-OPF constraints hold. Details on the construction of net load redistribution attack can be found in [27].

B. Moving Target Defense

MTD in power systems provides proactive defense in contrast to the traditional remedial defense approaches. As opposed to the MTD in the cyber communication network, MTD in the physical layer of power systems is extremely challenging as a small perturbation may deviate the system steady-state operating point from its optimal one.

The upper box with solid lines in Fig. 2 shows an MTD-enabled power system measurement-control-loop in wide area monitoring, protection and control (WAMPAC). Attackers can eavesdrop the power system measurement data and inject the manipulated measurement back to the system. If the attackers have the knowledge of the system configuration, they can construct and inject stealthy FDI attack vector M_a into the SCADA system. M_a can bypass an AC state estimation based BDD [28] if there is no MTD activated. The manipulated measurement (e.g., load $\hat{P}_d, \hat{Q}_d$) will be used in the applications of energy management systems, including the security constrained unit commitment and AC-OPF based economic dispatch P_G, Q_G. When an MTD is activated, the attacker's knowledge about the system configuration $h(\bullet)$ will be outdated and the injected attack vector that constructed based on the outdated $h(\bullet)$ can be detected by BDD. In this case, further investigation can be conducted to identify the attack vector under some conditions [14].

C. Power Injection to Impedance Sensitivity

The power injection to impedance (PII) sensitivity is originally proposed, as an intermediate step in the chain rule of calculus, to determine the relationship between the state variables and line impedance [29]. In this paper, the PII is utilized to calculate how much the system load margin can be increased due to the adjustment of the original MTD setpoints, when the system is near the power flow singularity (i.e., CPF nose point). The sensitivities of power injections to a change in line impedance is denoted as:

$$\begin{bmatrix} \Delta p \\ \Delta q \end{bmatrix} = [PII]\,[\Delta x_{ij}] \tag{1}$$

$$PII \triangleq \begin{bmatrix} \frac{\partial p}{\partial x_{ij}} \\ \frac{\partial q}{\partial x_{ij}} \end{bmatrix} \tag{2}$$

The power injection at Bus i is differentiated with respect to x_{ij} for all lines that connect Bus i and the adjacent Buses j. With the help of PII, the necessary MTD setpoints adjustment can be calculated under the most stressful system condition.

D. Voltage Stability Index (t-index)

The CPF method uses an iterative process involving predictor and corrector steps that require high computational cost for large systems. A different strategy to represent the voltage instability is by using the minimum singular value (MSV) of the power flow Jacobian. Cui et al. [19] proposed a voltage stability margin index to quantify the power flow Jacobian nonsingularity. The proposed voltage stability index is derived from a sufficient condition for the nonsingularity of power flow Jacobian [30]. A voltage stability index t_i for each load bus i is defined as:

$$t_i = |V_i| - \sum_{j=1}^{n} \frac{|Z_{ij} S_j|}{|V_j|}, \quad i, j \in \mathcal{N} \tag{3}$$

where $|V|$ is the voltage magnitude, S is the apparent power injection, Z_{ij} is the bus impedance matrix element, and $\mathcal{N}$ is the set of n load buses. A larger t-index value indicates a better voltage stability performance at a load bus. Contrasted with the CPF method, the t-index calculation does not require an iterative process which could greatly save computational efforts for a large system. As opposed to the CPF method, the t-index method is more suitable when the system operator is only concerned about power flow Jacobian singularity, while the tracing of the power flow solution path is not necessary.

IV. Voltage-stability-constrained MTD framework

In this section, we propose two voltage stability constrained MTD methods, i.e., a t-index optimization method and a load margin constrained method, to ensure the system voltage stability with sufficient load margin.

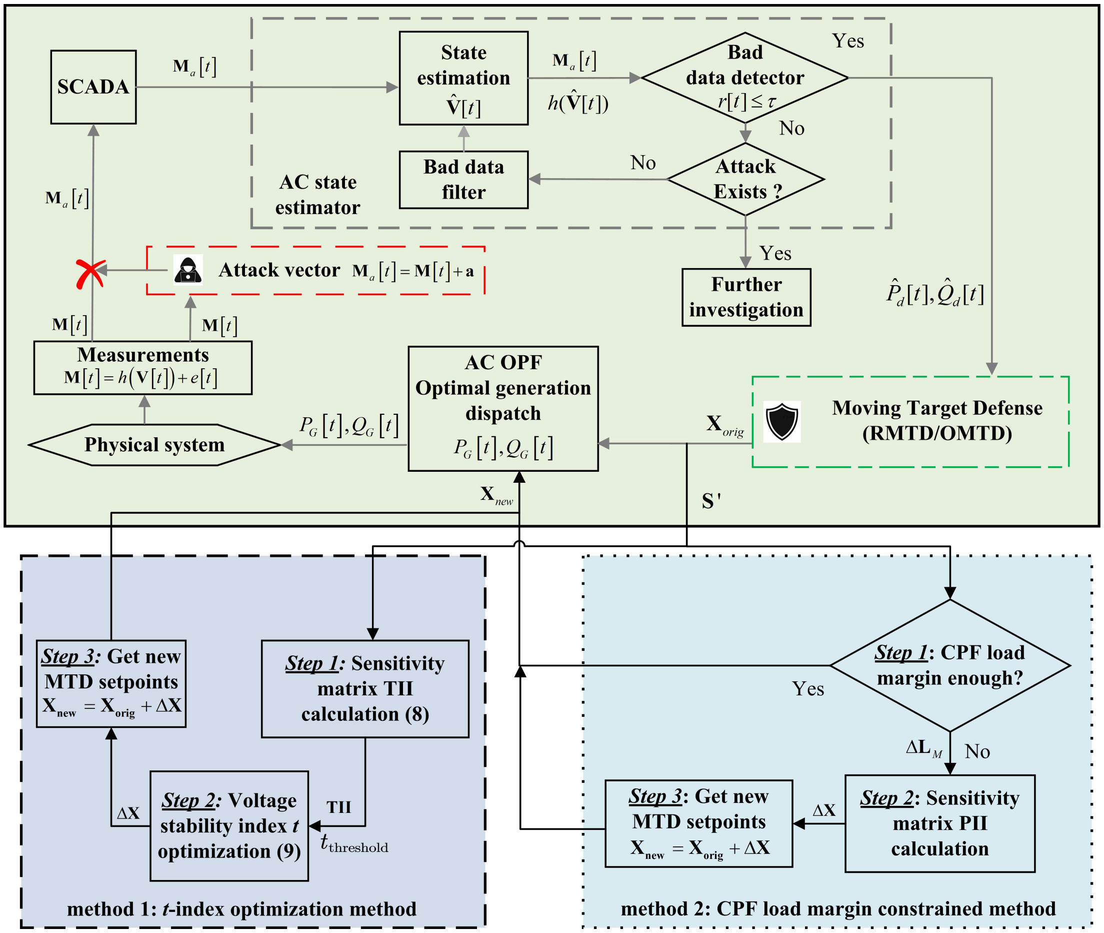

SCADA
$\mathbf{M}_a[t]$
State estimation $\hat{\mathbf{V}}[t]$
$\mathbf{M}_a[t]$
$h(\hat{\mathbf{V}}[t])$
Bad data detector $r[t] \le \tau$
Yes
No
Bad data filter
No
Attack Exists ?
AC state estimator
$\mathbf{M}_a[t]$
Attack vector $\mathbf{M}_a[t] = \mathbf{M}[t] + \mathbf{a}$
Yes
Further investigation
$\hat{P}_d[t], \hat{Q}_d[t]$
$\mathbf{M}[t]$
$\mathbf{M}[t]$
Measurements $\mathbf{M}[t] = h(\mathbf{V}[t]) + e[t]$
AC OPF Optimal generation dispatch $P_G[t], Q_G[t]$
$\mathbf{X}_{orig}$
Moving Target Defense (RMTD/OMTD)
Physical system
$P_G[t], Q_G[t]$
$\mathbf{X}_{new}$
S'
Step 3: Get new MTD setpoints $\mathbf{X}_{new} = \mathbf{X}_{orig} + \Delta\mathbf{X}$
Step 1: Sensitivity matrix TII calculation (8)
ΔX
Step 2: Voltage stability index t optimization (9)
TII
$t_{\text{threshold}}$
method 1: t-index optimization method
Step 1: CPF load margin enough?
Yes
$\Delta\mathbf{L}_M$
No
Step 3: Get new MTD setpoints $\mathbf{X}_{new} = \mathbf{X}_{orig} + \Delta\mathbf{X}$
ΔX
Step 2: Sensitivity matrix PII calculation
method 2: CPF load margin constrained method

Fig. 2. Flowchart of the new MTD framework with the proposed methods built-in.

A. *t-Index Optimization Method*

In this subsection, we first derive t-index to impedance sensitivity matrix (TII) and then form an optimization problem to maximize the t-index for the most critical forecasted load $S' = max([S_{t_1}, S_{t_2}, S_{t_3}, ..., S_{t_N}])$, where t_1 to t_N are the time indices of the look-ahead time periods within an MTD windows. The basic idea of the t-index optimization method is to maximize the lowest t-index among all the load buses of a system implemented with an original MTD. Our method is a post-MTD method that adjusts the original MTD setpoints.

1) TII Sensitivity Matrix: TII sensitivity matrix represents the relationship between the change of t-index ΔT and the change of MTD setpoints ΔX on the branches equipped with D-FACTS devices. The TII sensitivity matrix is described as follows:

$$\Delta T = TII \times \Delta X \tag{4}$$

$$TII \triangleq \left[\frac{\partial t_i}{\partial x_l}\right] = \left[\frac{\partial t_i}{\partial Z_{ij}} \times \frac{\partial Z_{ij}}{\partial x_l}\right], \quad i, j \in \mathcal{N}, \quad l \in \mathcal{L} \tag{5}$$

where TII is an $\mathcal{N} \times \mathcal{L}$ matrix, $\mathcal{L}$ is the set of D-FACTS equipped transmission lines l. From (3), it is shown that the t-indices at load buses are functions of the bus impedance matrix elements. To get the derivative of the t-index, the t-index at each load bus i is firstly differentiated with respect to the bus impedance matrix Z. Then, chain rule can be used to combine $\partial t_i/\partial Z_{ij}$ with $\partial Z_{ij}/\partial x_l$. During the derivative of t-index, the net power injection can be assumed as constant. Thus, t is a function of Z and V, $t_i = f(Z, V)$. For each load bus i, the derivative of t_i over Z is calculated by

$$\begin{aligned}
\frac{\partial t_i}{\partial Z_{ij}} &= \frac{\partial |V_i|}{\partial Z_{ij}} - \frac{1}{2}\sum_{j=1}^{n}\left(\frac{Z_{ij}S_jZ_{ij}^*S_j^*}{V_jV_j^*}\right)^{-\frac{1}{2}} \frac{\partial}{\partial Z_{ij}}\left(\frac{Z_{ij}S_jZ_{ij}^*S_j^*}{V_jV_j^*}\right) \\
&= \frac{\partial |V_i|}{\partial Z_{ij}} - \frac{1}{2}\sum_{j=1}^{n}\left(\frac{Z_{ij}S_jZ_{ij}^*S_j^*}{V_jV_j^*}\right)^{-\frac{1}{2}} S_jS_j^* \frac{\partial}{\partial Z_{ij}}\left(\frac{Z_{ij}Z_{ij}^*}{V_jV_j^*}\right) \\
&= \frac{\partial |V_i|}{\partial Z_{ij}} - \frac{1}{2}\sum_{j=1}^{n}\frac{|S_j|}{|Z_{ij}|\,|V_j|}\left(\frac{\partial\left(Z_{ij}Z_{ij}^*\right)}{\partial Z_{ij}} - \frac{|Z_{ij}|^2}{|V_j|^2}\frac{\partial\left(V_jV_j^*\right)}{\partial Z_{ij}}\right)
\end{aligned} \tag{6}$$

Note that for complex number C, $|C|^2 = CC^*$ holds, where C^* is the conjugate of C. For a normal complex derivative, Z_{ij}^* is not differentiable. This is because, for a complex limit calculation, a conjugate function variable can approach zero from different directions in the complex domain and results in different solutions, which is against the Cauchy–Riemann equations. Since $X \gg R$ in transmission systems, the line resistance can be ignored, and assume Z consists of pure imaginary variables. Then, we have $\frac{dZ_{ij}^*}{dZ_{ij}} = -1$ and

$$\frac{\partial t_i}{\partial Z_{ij}} = \frac{\partial |V_i|}{\partial Z_{ij}} + \sum_{j=1}^{n}\frac{|S_j|}{|V_j|} + \sum_{j=1}^{n}\frac{|S_j|\,|Z_{ij}|}{|V_j|^2}\frac{\partial |V_j|}{\partial Z_{ij}} \tag{7}$$

$\partial |V_i| / \partial Z_{ij}$ in (7) will turn to $\partial |V_i| / \partial x_l$ after the chain rule (5). Since the derivative of voltage magnitude over line impedance is equivalent to the state to impedance (SI) sensitivity in [29], $\partial |V_i| / \partial x_l$ can be replaced with the SI elements. The $(i,l)^{th}$ element in TII matrix can be calculated as,

$$\begin{aligned} TII_{il} &= \left[\frac{\partial t_i}{\partial x_l}\right] \\ &= SI_{il} + \sum_{j=1}^{n} \frac{|S_j|}{|V_j|}\frac{\partial Z_{ij}}{\partial x_l} + \sum_{j=1}^{n} \frac{|S_j|\,|Z_{ij}|}{|V_j|^2} SI_{il} \end{aligned} \tag{8}$$

For each transmission line equipped with D-FACTS devices, $\partial Z_{ij}/\partial x_l$ is calculated with respect to a unit step impedance change Δx_l.

2) t-Index Optimization Model: Based on the aforementioned TII sensitivity matrix, we further propose a t-index maximization model (9) to adjust the MTD setpoints. To facilitate the presentation, let subscript $orig$ denote an original post-MTD system state without using any voltage stability enhancement methods, and subscript new represent the state adjusted by using the proposed voltage stability methods. As original MTD operation methods optimize D-FACTS setpoints to achieve MTD hiddenness, maximize attack detection effectiveness, minimize power generation costs, and to minimize system losses [**?**], any adjustment on the original MTD setpoints would deviate from the optimal values. Therefore, the proposed model (9) also minimizes the MTD setpoints adjustment for a minimal impact on the original MTD performance.

$$\min_{\Delta X, t_{\text{threshold}}} \quad \delta_1 \|\Delta X\|_2 - \delta_2 t_{\text{threshold}} \tag{9}$$

$$\text{s.t.} \quad t_{\text{threshold}} \leq T_{\text{orig}} + \Delta T \tag{9a}$$

$$\text{LB} \leq X_{\text{orig}} + \Delta X \leq \text{UB} \tag{9b}$$

$$\Delta T = TII \times \Delta X \tag{9c}$$

where ΔX is the MTD setpoint adjustment which will be added to the setpoints in the original MTD X_{orig}. The final output of the proposed model is the optimized setpoints $X_{\text{new}} = X_{\text{orig}} + \Delta X$. δ_1 and δ_2 are the weighted coefficients to balance the trade-off between the impact on the performance of the original MTD and the t-index increase. The first component of the objective function (9) minimizes the adjustment of the MTD branch impedance which ensures the adjustment will not significantly affect the performance of the original MTD. The second component of (9) maximizes (i.e., minimize negative) the t-index threshold $t_{\text{threshold}}$, which is equivalent to maximizing the t-index at the most critical load bus. T_{orig} is the vector of t-index in the system with the original MTD at the peak net load S'. Constraint (9a) is the t-index threshold constraint to ensure the lowest t at the most critical load bus is greater than the t-index threshold. Constraint (9b) aims to ensure the total impedance change after the adjustment is within the physical capacity of D-FACTS devices. LB and UB are the lower and upper bounds of line reactance perturbation, where UB and LB are equal to $\pm 20\%$ of the transmission line impedance which is generally used in MTD [5], [6], [8], [9], [11], [14]. In (9c), ΔT is the vector of the incremental t-index at all load buses calculated based on TII.

Algorithm 1 t-index optimization method

```
Input: $X_{\text{orig}}$, $S'$
Output: $X_{\text{new}}$
Calculate $TII$ from (8)
Solve the $t$-index optimization problem (9)
$X_{\text{new}} = X_{\text{orig}} + \Delta X$
return $X_{\text{new}}$
```

The steps of the proposed t-index optimization method are shown in Algorithm 1. In general, TII is calculated and the t-index optimization method is carried out for the most critical net load condition $S' = max([S_{t_1}, S_{t_2}, S_{t_3}, ..., S_{t_N}])$ within an MTD window between time t_1 and t_N. Since the proposed model (9) maximizes the t-index at the most critical load bus, the t-index at the load bus with high voltage stability may degrade. However, this is typically acceptable as the entire system remains voltage stable under the most stressful condition. Note that the weight coefficients can be finely tuned to find the trade-off between the MTD's performance and the voltage stability. For instance, when higher variability and uncertainty of renewable generation are considered, a higher weight can be placed on the voltage stability rather than maintaining a small impact on the original MTD's performance.

B. Load Margin Constrained Method

Load margin L_M is another noteworthy metric for measuring the system voltage stability. It is defined as the maximum amount of load that the system can support given a system configuration. With a specific system configuration and peak load forecast, the load margin is calculated by CPF with a predictor-corrector method. As previously discussed, all existing MTD methods fail to consider the system load margin that is very likely to degrade by MTDs. This motivates us to develop a load margin constrained MTD method. The proposed method is demonstrated in the dotted box of Fig. 2 and the steps, shown in Algorithm 2, are described as follows:

- *Step 1*: Algorithm 2 checks the original D-FACTS setpoints X_{orig} by using the CPF method. The load margin L_M is calculated given the original MTD and forecast peak load. If the load margin of X_{orig} is able to satisfy the most critical load forecast within an MTD window, i.e., $S' \leq L_M$, these setpoints can be applied to the system without adjustment. Otherwise, the expected incremental load margin can be calculated by $\Delta L_M = S' - L_M$.
- *Step 2*: Algorithm 2 computes the sensitivity matrix PII in (2). PII reveals the relationship between the expected incremental load margin ΔL_M and the line impedance change ΔX on the branches equipped with D-FACTS devices. After computing PII, Algorithm 2 calculates the expected MTD setpoint adjustment by $\Delta X = PII^{-1} \times \Delta L_M$. ΔX must ensure the MTD setpoint after the adjustment is still within the physical limits of the D-FACTS devices, i.e., LB $\leq X_{\text{orig}} + \Delta X \leq$ UB. LB and UB are the same as used in the t-index optimization method.
- *Step 3*: The load margin constrained MTD setpoints are calculated by adding ΔX to the original MTD setpoints,

Algorithm 2 load margin constrained method

```
Input: $X_{\text{orig}}$, $S'$
Output: $X_{\text{new}}$
 1: Solve CPF problem to get load margin $L_M$ of $X_{\text{orig}}$
 2: if $S' \leq L_M$ then (as they satisfy the load margin constraint for the most critical condition)
 3:     return $X_{\text{orig}}$
 4: else
 5:     Calculate the expected load margin increase $\Delta L_M$
 6:     Compute the $PII$ from (2)
 7:     Solve $\Delta X = PII^{-1} \times \Delta L_M$, subject to LB $\leq X_{\text{orig}} + \Delta X \leq$ UB
 8:     $X_{\text{new}} = X_{\text{orig}} + \Delta X$
 9: end if
10: return $X_{\text{new}}$
```

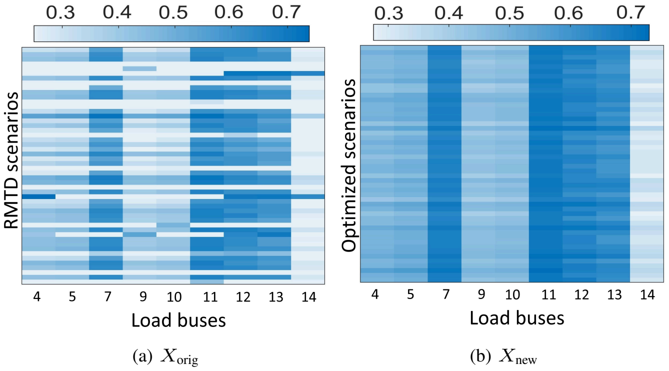
i.e., $X_{\text{new}} = X_{\text{orig}} + \Delta X$. The new MTD setpoints are then returned by Algorithm 2.

Notice that the scope of this paper is on the voltage stability issue induced by MTD only. In other words, the pre-MTD system state is voltage stable even under the most stressful conditions without MTD. In view of the MTD setpoint that is perturbed around the pre-MTD system state ΔL_M calculated in *Step 2* should be comparatively small. However, if the system is not pre-MTD voltage sable ΔL_M can be large. In such a case, feasible X_{new} may not exist due to the physical limits of the D-FACTS devices. Other methods [31], [32] including the potential load shedding as a last resort, need to be considered to ensure the pre-MTD voltage stability of the system.

C. Proposed Voltage Stability Constrained MTD Framework

Figure 2 illustrates the proposed flowchart of the voltage-stability constrained MTD framework that integrates Algorithm 1 and Algorithm 2 proposed in this section. These two methods lie in the post-MTD process where original MTD setpoints are calculated and can be adjusted if deemed necessary. Our core idea in designing this framework is that the proposed methods ought to greatly enhance the system voltage stability within an MTD rolling window, but should not significantly degrade the attack detection effectiveness of the original MTD setpoints or incur a prominent increase in the system operating cost.

By comparing the two proposed algorithms, the t-index optimization method has an advantage over the load margin constrained method that the adjusted MTD setpoints X_{new} are typically closer to the original MTD setpoints X_{orig} since the minimization of the setpoint deviation in (9). This is much desirable when the original MTD is an OPF-based MTD strategy (e.g., OMTD and HMTD) with specific objectives including system cost minimization, attack detection probability maximization, and/or MTD hiddenness requirement. The t-index optimization method can improve the voltage stability while maintaining the original OMTD performance as much as possible. Both of the proposed methods are computationally efficient since they only involve matrix computations, solving a series of power flow problems, and solving a nonlinear minimization problem with all linear constraints. Our numerical tests show that the proposed methods can solve an IEEE 118-bus case with 60 D-FACTS devices within 20 seconds on a desktop computer. More comparative numerical results will be shown in the next section.



(a) X_{orig}

(b) X_{new}

Fig. 3. t-indices before and after the t-index optimization method in the 14-bus system

V. Numerical results

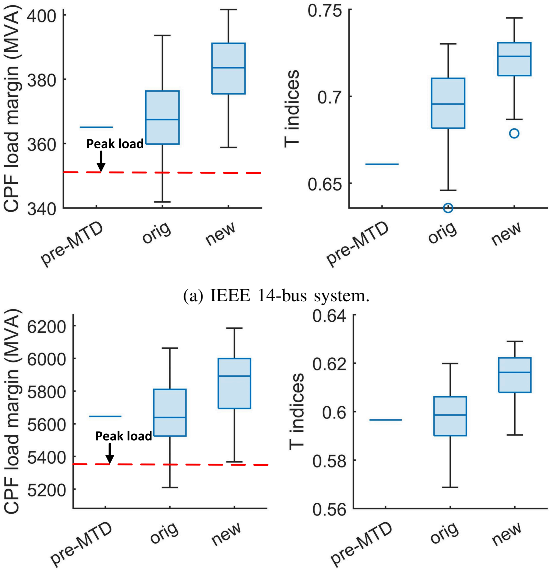
In this section, we present the case study and simulation results on the proposed methods and framework. The net load redistribution attack against MTD detection cases are tested on the IEEE 14-bus and 118-bus systems available from MATPOWER [33]. The t-index optimization problem is solved by the FMINCON toolbox in MATLAB. The load margin constrained method is implemented by using the CPF toolbox in MATPOWER. In order to compare the performance of the proposed methods with various MTDs, we use two MTD placement methods, i.e., max-rank [5] and graph-based placement [12], as well as two MTD operational strategies, i.e., RMTD and OMTD in the case study. The simulations are performed on a desktop with an Intel Core i5 processor and 8 GB RAM. The line impedance change in all the cases are set to be within 20% of the original impedance.

A. Impact on Voltage Stability Metrics

To compare and evaluate the performance of the two proposed methods, we construct 1000 RMTDs to form a defense pool. We scale up the load of the two systems by 1.35 times to create a very stressful load condition. Figure 3 shows the heat-maps that compare the t-indices of all the load buses in the IEEE 14-bus system with the original MTD (Fig. 3(a)), and with the new t-index optimized MTD (Fig. 3(b)). In this figure, each row represents one RMTD from the defense pool, while each column represents a load bus in this system. By examining all the RMTDs in the defense pool, it is found that 16% of the original RMTDs undergo voltage collapse at the peak load. In comparison, all the failed cases are saved from voltage collapse by implementing the t-index optimization method. The t-indices in Fig. 3(b) indicates that the proposed t-index optimization method significantly increases the capability of voltage support of the systems with the original MTD.

Figure 4 demonstrates the box plot of two voltage stability metrics, i.e., load margin and the minimum t-indices value, for all the load buses in the two systems before and after implementing the proposed t-index optimization method. In each box, the central mark indicates the median, and the bottom and top edges suggest the 25th and 75th percentiles, respectively. The whiskers extend to the most extreme data points exclude outliers, and the outliers are plotted individually. Three system states are compared including the pre-MTD state, the original MTD state, and the new MTD state. It is observed that when the system is transitioning from pre-MTD to original MTD state, the CPF load margin and the t-indices may increase or decrease. This is because the RMTDs in the defense pool are constructed randomly without considering the voltage stability. As seen, from the original to new MTD state, the proposed t-index optimization method elevates both the t-indices and the CPF load margin, indicating increased system voltage stability. A similar trend, shown in Fig. 4(b) can be observed in the IEEE 118-bus system. Two peak loads are labeled as dashed red lines in the load margin figures. These peak loads, which are not used here in Algorithm 1, are added to be consistent with Fig. 5. The results in Fig. 4 show that the t-index optimization method can promote both of those metrics, which in turn increase the voltage stability of the system.

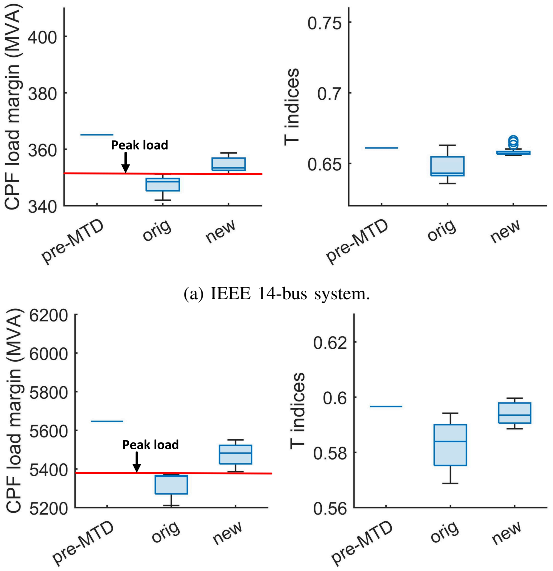
Analogously, Fig. 5 shows the box plots of those voltage stability metrics before and after using the proposed load margin constrained method. According to Algorithm 2, this method only makes adjustment if the system cannot support the forecasted peak load. Therefore, Fig. 5 only shows the original MTDs that fail to do so, which is why the body of the box plot in Fig. 5 is much shorter than that in Fig. 4. In the IEEE 14-bus system, the forecasted peak load is 351.2 MVA labeled by a horizontal red line. In the left plot of Fig. 5(a), the load margin of the pre-MTD state is 365.1 MVA, which is greater than the forecasted peak load. Hence, the pre-MTD system state is capable of supporting the forecasted peak load. For all RMTDs whose original load margin is less than the forecasted peak load (i.e., “problematic” RMTDs), Lines 5-10 in Algorithm 2 are executed. It is seen in the left plot of Fig. 5(a) that the proposed load margin constrained method significantly brings up the load margin of those problematic RMTDs. As a result, the load margin of all new MTDs are equal to or greater than the forecasted peak load. The right plots in Fig. 5(a) shows the minimum values of t-indices among all the load buses. As seen, the t-indices of the system also increase by using the proposed load margin constrained method. Nevertheless, the improvement is not as significant as that in Fig. 4(a) since the t-indices are not directly maximized in the load margin constrained method. Similar plots for the IEEE 118-bus system are displayed in Fig. 5(b). The results in Fig. 5 demonstrate that the proposed load margin constrained method can significantly increase the load margin of original MTDs and ensure ample load margins to support the forecasted peak load.



(a) IEEE 14-bus system.

(b) IEEE 118-bus system.

Fig. 4. Voltage stability metrics before and after t-index optimization method



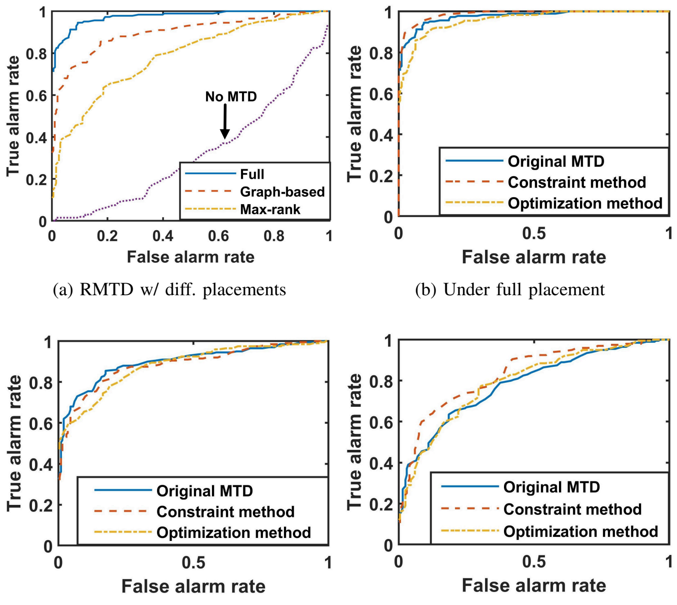
(a) IEEE 14-bus system.

(b) IEEE 118-bus system.

Fig. 5. Voltage stability metrics before and after load margin constrained method

B. Impact on Generation Cost and Attack Detection

In this subsection, we evaluate the impact of the two proposed methods on the system generation cost and MTD performance with various MTD settings. Table I illustrates the system generation costs for the peak load in four cases. The ACOPF in MATPOWER is used to optimally dispatch the generation for each case as illustrated in Fig. 2. In Table I, the first case shows the pre-MTD generation cost of the systems, while the second case represents the original-MTD generation cost when an ACOPF-based OMTD [5] is executed. The last two cases show the new-MTD generation costs after each proposed method is implemented. As seen, for both the IEEE 14-bus and 118-bus systems, the lowest generation costs are associated with the OMTD operation in the original MTD state. This is expected since the OMTD operation without considering the voltage stability is solely dedicated to the cost minimization. The second lowest generation costs are pertaining to the new MTD state after the t-index optimization method is implemented. A relatively small cost increase is induced by this method. This is because the t-index optimiza-



(a) RMTD w/ diff. placements

(b) Under full placement

(c) Under graph-based placement

(d) Under max-rank placement

Fig. 6. ROC curves of BDD residual in IEEE 118-bus system.

tion method optimally adjusts the original OMTD setpoints to improve the t-indices of load buses and the resulting new MTD setpoints are close to the OMTD ones. The largest generation cost emerges when the load margin constrained method is applied due to much larger MTD setpoint deviation from the OMTD ones. The generation cost results in Table I show that the load margin method is able to guarantee the system voltage stability at a higher system generation cost. In contrast, the t-index optimization method can ensure the voltage stability with a negligible increase in system generation cost.

Furthermore, simulations are carried out to test the MTD effectiveness against net load redistribution attacks using AC SE-based BDD. Four different D-FACTS placements are considered including zero placement (No-MTD), full placement, max-rank placement [5], and graph-based placement [12]. The measurement noise is assumed to be Gaussian distributed with zero mean and the standard deviation as 1% of the actual measurement. For each MTD placement, we again construct 1,000 RMTDs as the corresponding defense pool. We further construct 1,000 net load redistribution attack vectors to form an attack pool. Figure 6 shows the receiver operating characteristic (ROC) curves of MTDs. These ROC curves are created by plotting the true positive rate (TPR) versus the false positive rate (FPR) at various BDD thresholds. Figure 6(a) compares the attack detection effectiveness of the original MTD under different MTD placements. As seen, , the ROC curve without MTD passes through the bottom right of the graph, leading to the smallest area under the curve (AUC) among all the placement. A smaller AUC indicates a worse performance in attack detection effectiveness. Again, the results in Figure 6(a) demonstrates: 1) the net load redistribution attack is stealthy against AC SE-based BDD; 2) instead of increasing the BDD residual, the net load redistribution attack decreases the residual [27], leading to a smaller TPR than the FPR at a given threshold; and 3) the attack detection effectiveness is related to the numbers of D-FACTS devices deployed. The more D-FACTS devices deployed, the higher attack detection effectiveness would be.

TABLE I
Comparison of Generation Costs at the Peak Load

Cases	14-bus ($/hr)	118-bus ($/hr)
Pre-MTD	8,083.2	129,725.8
OMTD operation	8,076.4	129,714.6
Constrained method	8,358.0	129,906.3
Optimization method	8,083.9	129,718.8

Further, we test the impacts of the two proposed methods on the attack detection effectiveness under the other three D-FACTS placements, whose attack detection effectiveness is compared in Figs. 6(b) to 6(d). It is seen that both the load margin constrained method and the t-index optimization method will maintain similar attack detection effectiveness as the original RMTD under the full and graph-based MTD placement. A larger AUC difference between the original MTD and the load margin constrained MTD emerges under the max-rank placement. This can be explained by examining the line impedance change in percentage induced by an MTD, which is indicative of the average absolute MTD magnitude. The average MTD magnitudes of the load margin constrained MTD is 10.42% which is larger than that of the other two MTDs, i.e., 9.70%. Here, the observation that the attack detection effectiveness increases with the MTD magnitude is consistent with other MTD works [7], [24]. The results in Fig. 6(b) to 6(d) indicate that both of the proposed methods can maintain similar attack detection effectiveness as the original MTD. Moreover, by minimizing the MTD adjustment in (9), the t-index optimization method has a relatively smaller impact on the attack detection effectiveness performance of the original MTD compared with the load margin method.

VI. Conclusion

In this paper, we address a critical issue induced by existing MTDs that myopically perturb the transmission line impedance and result in system voltage instability for varying (net) load. A 3-bus example system is used as an example to illustrate this issue and two methods are further proposed to address it. For the first method, namely the t-index optimization method, we derive the t-index to impedance sensitivity matrix. By utilizing this matrix, we maximize the lowest t among all the load buses with the minimum impedance adjustment such that the system voltage stability is guaranteed while keeping the performance of the original MTD strategy. The second method, i.e., a load margin constrained method, is developed based on CPF to ensure the load margin is beyond the forecast peak load and thus keeps the system voltage stable during the most stressful time period. Furthermore, we propose a new MTD framework that seamlessly integrates the proposed two methods.

Extensive simulation results show that both methods can greatly improve the load margin and the voltage stability of a system with an original MTD in critical net load conditions. Moreover, the t-index optimization method can maintain the objectives close enough to the original OMTDs. The load margin constrained method may induce the new MTD setpoints further away from the original MTD, which is acceptable when RMTD is originally implemented. In reality, system operators can choose either of the two proposed methods to enhance the system voltage stability for RMTDs. When OMTD is originally implemented in the system, a better choice is the t-index optimization method. In future work, we will explore implementing the proposed MTD voltage stability constrained methods under other advanced MTD strategies including inverter-based MTDs to equivalently change system configurations.

Acknowledgment

This material is based upon work supported in part by the U.S. National Science Foundation under Grant No. 1929147, and in part by the U.S. Department of Energy under Award No. DE-EE0008767.

References

[1] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29 641–29 659, 2021.

[2] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2019.

[3] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012, pp. 342–347.

[4] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *2012 45th Hawaii International Conference on System Sciences*. IEEE, 2012, pp. 2104–2113.

[5] B. Liu and H. Wu, "Optimal D-FACTS placement in moving target defense against false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4345–4357, 2020.

[6] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2208–2223, 2018.

[7] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, "Moving target defense approach to detecting stuxnet-like attacks," *IEEE transactions on smart grid*, vol. 11, no. 1, pp. 291–300, 2019.

[8] B. Liu, H. Wu, A. Pahwa, F. Ding, E. Ibrahim, and T. Liu, "Hidden moving target defense against false data injection in distribution network reconfiguration," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2018, pp. 1–5.

[9] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using d-facts devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 854–864, 2019.

[10] "A Mobile Unit Tours Europe, Smart Wires in India and More." [Online]. Available: https://www.smartwires.com/portfolio-item/8245/

[11] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proceedings of the First ACM Workshop on Moving Target Defense*, 2014, pp. 59–68.

[12] B. Liu and H. Wu, "Systematic planning of moving target defence for maximising detection effectiveness against false data injection attacks in smart grid," *IET Cyber-Physical Systems: Theory & Applications*, 2021.

[13] S. Lakshminarayana and D. K. Yau, "Cost-benefit analysis of moving-target defense in power grids," *IEEE Transactions on Power Systems*, 2020.

[14] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying FDI attacks in power system state estimation," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 763–776, 2018.

[15] M. Cui and J. Wang, "Deeply hidden moving-target-defense for cyber-secure unbalanced distribution systems considering voltage stability," *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 1961–1972, 2021.

[16] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense for detecting coordinated cyber-physical attacks in power grids," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2019, pp. 1–7.

[17] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal, "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1387–1401, 2004.

[18] L. Wang and H.-D. Chiang, "Toward online line switching for increasing load margins to static stability limit," *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 1744–1751, 2015.

[19] B. Cui and X. A. Sun, "A new voltage stability-constrained optimal power-flow model: Sufficient condition, SOCP representation, and relaxation," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5092–5102, 2018.

[20] C. Wang, B. Cui, Z. Wang, and C. Gu, "SDP-based optimal power flow with steady-state voltage stability constraints," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4637–4647, 2018.

[21] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2320–2335, 2020.

[22] M. Higgins, K. Mayes, and F. Teng, "Enhanced cyber-physical security using attack-resistant cyber nodes and event-triggered moving target defence," *arXiv preprint arXiv:2010.14173*, 2020.

[23] V. Ajjarapu and C. Christy, "The continuation power flow: a tool for steady state voltage stability analysis," *IEEE Transactions on Power Systems*, vol. 7, no. 1, pp. 416–423, 1992.

[24] B. Liu and H. Wu, "Optimal planning and operation of hidden moving target defense for maximal detection effectiveness," *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.

[25] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[26] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 6 2011.

[27] H. Zhang, B. Liu, and H. Wu, "Net load redistribution attacks on nodal voltage magnitude estimation in ac distribution networks," in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 2020, pp. 46–50.

[28] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[29] K. M. Rogers and T. J. Overbye, "Some applications of distributed flexible AC transmission system (D-FACTS) devices in power systems," in *2008 40th North American Power Symposium*, 2008, pp. 1–8.

[30] Z. Wang, B. Cui, and J. Wang, "A necessary condition for power flow insolvability in power distribution systems with distributed generators," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1440–1450, 2017.

[31] R. Faranda, A. Pievatolo, and E. Tironi, "Load shedding: A new proposal," *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 2086–2093, 2007.

[32] C. Mozina, "Undervoltage load shedding," in *2007 Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources*, 2007, pp. 39–54.

[33] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.